

(19)



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2000101567 A**

(43) Date of publication of application: **07.04.00**

(51) Int. Cl.

H04L 9/26
G09C 1/00

(21) Application number: **10263681**

(71) Applicant: **TOYO COMMUN EQUIP CO LTD**

(22) Date of filing: **17.09.98**

(72) Inventor: **SUGIMOTO KOICHI**

(54) CIPHERING AND DECIPHERING DEVICE AND METHOD THEREFOR

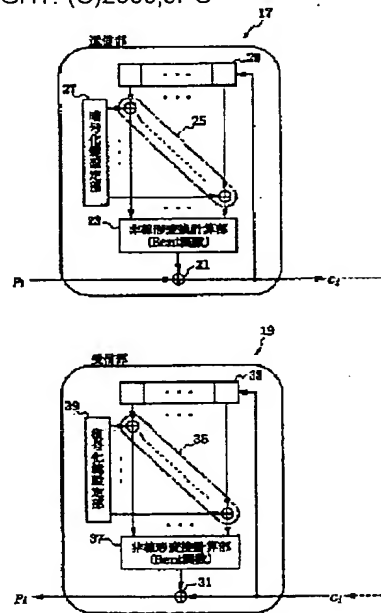
(57) Abstract:

PROBLEM TO BE SOLVED: To make cross correlation extremely small in the case of comparing a sequence in the case of deciphering the sequence of a cipher sentence by a certain key by a different key with the sequence of a plain sentence and to easily set a key.

SOLUTION: This device is provided with the first shift register 29 of plural stages operated in synchronism with synchronizing signals, the nonlinear transformation calculation part 23 of multi-bit input and 1-bit output, a cipher key setting part 27, an exclusive OR means 25 for exclusively ORing a cipher key set in the cipher key setting part to the register value of the shift register for respective bits and supplying it to the nonlinear transformation calculation part and the exclusive OR means 21 for exclusively ORing the plain sentence and the output of the nonlinear transformation calculation part for the respective bits. The nonlinear transformation calculation part

is provided with the Boolean function computation means of the multi-bit input and 1-bit output called as a Bent function.

COPYRIGHT: (C)2000,JPO



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-101567

(P2000-101567A)

(43) 公開日 平成12年4月7日(2000.4.7)

(51) Int. Cl. ⁷	識別記号	F I	キーワード(参考)
H 0 4 L 9/26		H 0 4 L 9/00	6 5 9 5 J 1 0 4
G 0 9 C 1/00	6 1 0	G 0 9 C 1/00	6 1 0 D

審査請求 未請求 請求項の数 4 O L (全 7 頁)

(21) 出願番号 特願平10-263681

(22) 出願日 平成10年9月17日(1998.9.17)

(71) 出願人 000003104

東洋通信機株式会社

神奈川県高座郡寒川町小谷2丁目1番1号

(72) 発明者 杉本 浩一

神奈川県高座郡寒川町小谷2丁目1番1号

東洋通信機株式会社内

(74) 代理人 100085650

弁理士 鈴木 均

Fターム(参考) 5j104 A4G1 A418 J406 N4G2 N408

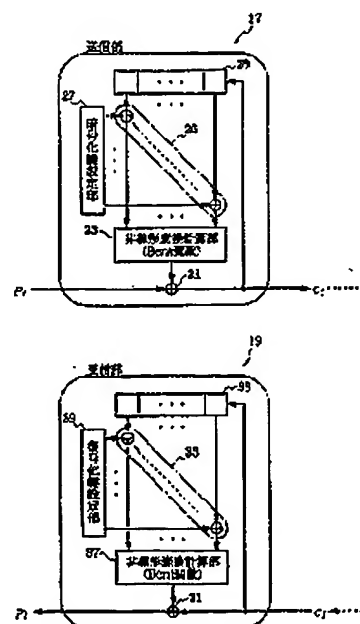
NA23

(54) 【発明の名称】 暗号化及び復号化装置とその方法

(57) 【要約】 (修正有)

【課題】 ある鍵による暗号文の系列を異なる鍵で復号した場合の系列を、平文の系列と比較した場合、相互相関が極めて小さく、かつ、鍵の設定を容易にする。

【解決手段】 同期信号に同期して動作する複数段の第1のシフトレジスタ29と、多ビット入力1ビット出力の非線形変換計算部23と、暗号化鍵設定部27と、シフトレジスタのレジスタ値に対して上記暗号化鍵設定部に設定された暗号化鍵をビット毎に排他的論理和演算して非線形変換計算部へ供給する排他的論理和演算手段25と、平文と非線形変換計算部の出力とをビット毎に排他的論理和演算する排他的論理和演算手段21とを具備し、非線形変換計算部はBent関数と呼ばれる多ビット入力1ビット出力のブール関数演算手段を備える。



(2)

特開2000-101567

1

2

【特許請求の範囲】

【請求項1】 伝送情報（平文）を暗号化する暗号化装置であって、同期信号に同期して動作する複数段のシフトレジスタと、多ビット入力1ビット出力の非線形変換計算部と、暗号化鍵設定部と、上記シフトレジスタの一部もしくは全部のレジスタ値に対して上記暗号化鍵設定部に設定された暗号化鍵をビット毎に排他的論理和演算して上記非線形変換計算部へ供給するための第1の排他的論理和演算手段と、上記平文と上記非線形変換計算部からの出力とをビット毎に排他的論理和演算するための第2の排他的論理和演算手段とを具備し、
上記非線形変換計算部は、少なくともBent関数と呼ばれる多ビット入力1ビット出力のブール関数演算手段を備えたものであり、暗号文が、上記平文と上記非線形変換計算部からの出力とをビット毎に排他的論理和演算することによって得られ、その暗号文が、同時に上記シフトレジスタに入力される構成となっていることを特徴とする自己同期型ストリーム暗号化装置。

【請求項2】 暗号文を復号化する復号化装置であって、同期信号に同期して動作する複数段のシフトレジスタと、多ビット入力1ビット出力の非線形変換計算部と、復号化鍵設定部と、上記シフトレジスタの一部もしくは全部のレジスタ値に対して上記復号化鍵設定部に設定された復号化鍵をビット毎に排他的論理和演算して上記非線形変換計算部へ供給するための第1の排他的論理和演算手段と、上記暗号文と上記非線形変換計算部からの出力とをビット毎に排他的論理和演算するための第2の排他的論理和演算手段とを具備し、
上記非線形変換計算部は、少なくともBent関数と呼ばれる多ビット入力1ビット出力のブール関数演算手段を備えたものであり、上記暗号文が、上記シフトレジスタに入力され、同時に、平文が、先の暗号文と非線形変換計算部からの出力とをビット毎に排他的論理和演算を施すことによって得られることを特徴とする自己同期型ストリーム復号化装置。

【請求項3】 伝送情報（平文）を暗号化する暗号化方法であって、同期信号に同期して動作する複数段のシフトレジスタの一部もしくは全部のレジスタ値に対して暗号化鍵設定部に設定された暗号化鍵を第1の排他的論理和演算手段によりビット毎に排他的論理和演算するステップと、
少なくともBent関数と呼ばれる多ビット入力1ビット出力のブール関数演算手段を備えた非線形変換計算部によって上記第1の排他的論理和演算手段よりの値を非線形変換するステップと、
上記平文と上記非線形変換計算部からの出力とを第2の排他的論理和演算手段によりビット毎に排他的論理和演算するステップと、
上記暗号文を上記シフトレジスタに入力するステップとを具備することを特徴とする自己同期型ストリーム暗号

化方法。

【請求項4】 暗号文を復号化する復号化方法であって、同期信号に同期して動作する複数段のシフトレジスタの一部もしくは全部のレジスタ値に対して復号化鍵設定部に設定された復号化鍵を第1の排他的論理和演算手段によりビット毎に排他的論理和演算するステップと、
少なくともBent関数と呼ばれる多ビット入力1ビット出力のブール関数演算手段を備えた非線形変換計算部によって上記第1の排他的論理和演算手段よりの値を非線形変換するステップと、
上記暗号文と上記非線形変換計算部からの出力とを第2の排他的論理和演算手段によりビット毎に排他的論理和演算するステップと、
上記暗号文を、上記シフトレジスタに入力するステップとを具備することを特徴とする自己同期型ストリーム復号化方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、伝送情報（平文）を暗号化して通信する暗号通信システムに関し、特に、ある鍵によって生成された暗号文の系列を異なる鍵で復号した場合の系列と平文の系列とを比較した場合、その相互相関が極めて小さくなり、かつ、鍵の設定が容易となる自己同期型ストリーム暗号方式の暗号通信システムにおける暗号化及び復号化装置とその方法に関する。

【0002】

【従来の技術】従来より、電話機や無線通信装置やデータ通信装置等における暗号通信システムにおいては、その暗号通信システムの両端の通信当事者以外の第三者がその暗号通信システムで伝送される情報を知ることができないようにするために、その暗号通信システムで伝送される伝送情報を暗号化することが行われている。この暗号化の方式としては多種の方式が知られているが、高速なデータ通信に利用可能な方式としてはストリーム暗号方式が知られている。以下に、ストリーム暗号方式の一形態である自己同期型ストリーム暗号方式について図3に示す暗号通信システムを例にあげて説明する。図3において、この暗号通信システムは、データストリーム（平文）を暗号化する自己同期型ストリーム暗号化方式の送信部1および暗号化されたストリーム（暗号文）を復号する自己同期型ストリーム復号化方式の受信部3とを有している。上記送信部1と受信部3とは互いに同形状の第1および第2のシフトレジスタ5、7を有し、同形状の第1および第2の非線形変換計算部9、11を共有している。すなわち、上記送信部1では、平文P₁を入力する第1の排他的論理和演算部13に第1の非線形変換計算部9が接続され、上記第1の非線形変換計算部9に第1のシフトレジスタ5が接続され、上記第1の排他的論理和演算部13の出力C₁が伝送されると共に上記第1のシフトレジスタ5に入力される構成となってお

(3)

特開2000-101567

3

り、上記受信部3では、上記出力C_iを入力する第2の排他的論理和演算部15および第2のシフトレジスタ7の間に第2の非線形変換計算部11が接続される構成となっている。

【0003】次に、上記暗号通信システムにおける暗号通信動作について説明する。まず、上記送信部1は、平文P_iをビット毎に入力すると同期信号に同期して暗号文C_iがビット毎に出力される様になっている。すなわち、詳細に説明すると、上記平文P_iと第1の非線形変換計算部9の出力とは上記第1の排他的論理和演算部13でビット毎に排他的論理和演算を施され、その結果は暗号文C₁として出力されると共に、上記第1のシフトレジスタ5の最右段に入力される。上記第1のシフトレジスタ5は同期信号に同期してその記憶されている内容を1ビット左シフトし、上記第1の非線形変換計算部9は上記第1のシフトレジスタ5の各段におけるレジスタ値を非線形変換し、結果の1ビットを出力する。一方、上記受信部3は、上記送信部1から送信された暗号文C₁をビット毎に入力すると同期信号に同期して平文P₁がビット毎に出力される様になっている。すなわち、暗号文C₁と上記第2の非線形変換計算部11の出力とは上記第2の排他的論理和演算部15でビット毎に排他的論理和演算を施され、その結果は平文P₁として出力されると同時に、暗号文C_iは、上記第2のシフトレジスタ7の最右段に入力される。上記第2のシフトレジスタ7は同期信号に同期してその記憶されている内容を1ビット左シフトし、上記第2の非線形変換計算部11は上記第2のシフトレジスタ7の各段におけるレジスタ値を非線形変換し、結果の1ビットを出力する。

【0004】

【発明が解決しようとする課題】しかしながら、上記図3に示す自己同期型ストリーム暗号方式の暗号通信システムでは、暗・復号化鍵として、上記非線形変換計算部9、11の形状を共有する必要がある。その構造は複雑で暗・復号化鍵として扱いづらいという問題があった。また、鍵同士には、ある鍵によって生成された暗号文の系列を異なる鍵で復号した場合の系列と平文の系列とを比較した場合、その相互相関が極めて小さくなければならない性質が要求される。すなわち、暗号解読の難易度を高くするためには、鍵同士には、復号化の鍵が暗号化鍵と異なった場合、平文と全く異なった系列が生じることが必要となる。しかるに、このような性質をもった非線形変換計算部を鍵として採択する効率的な手法が存在しないといった問題があった。本発明は、上記問題に鑑みてなされたものであって、ある鍵によって生成された暗号文の系列を異なる鍵で復号した場合の系列と平文の系列とを比較した場合、その相互相関が極めて小さくなり、かつ、鍵の設定が容易となる自己同期型ストリーム暗号方式の暗号化及び復号化装置とその方法を提供することを目的とする。

4

【0005】

【課題を解決するための手段】上記目的を達成するために、本発明は、伝送情報（平文）を暗号化する自己同期型ストリーム暗号化装置において、同期信号に同期して動作する複数段のシフトレジスタと、多ビット入力1ビット出力の非線形変換計算部と、暗号化鍵設定部と、上記シフトレジスタの一部もしくは全部のレジスタ値に対して上記暗号化鍵設定部に設定された暗号化鍵をビット毎に排他的論理和演算して上記非線形変換計算部へ供給するための第1の排他的論理和演算手段と、上記平文と上記非線形変換計算部からの出力とをビット毎に排他的論理和演算するための第2の排他的論理和演算手段とを具備し、上記非線形変換計算部は、少なくともBen_t関数と呼ばれる多ビット入力1ビット出力のブール関数演算手段を備えたものであり、暗号文が、平文と上記非線形変換計算部からの出力とをビット毎に排他的論理和演算することによって得られ、その暗号文が、同時に上記シフトレジスタに入力される構成となっていることを特徴とする。

【0006】本発明の他の特徴は、暗号文を復号化する自己同期型ストリーム復号化装置において、同期信号に同期して動作する複数段のシフトレジスタと、多ビット入力1ビット出力の非線形変換計算部と、復号化鍵設定部と、上記シフトレジスタの一部もしくは全部のレジスタ値に対して上記復号化鍵設定部に設定された復号化鍵をビット毎に排他的論理和演算して上記非線形変換計算部へ供給するための第1の排他的論理和演算手段と、暗号文と上記非線形変換計算部からの出力とをビット毎に排他的論理和演算するための第2の排他的論理和演算手段とを具備し、上記非線形変換計算部は、少なくともBen_t関数と呼ばれる多ビット入力1ビット出力のブール関数演算手段を備えたものであり、上記暗号文が、上記シフトレジスタに入力され、同時に、上記平文が、先の暗号文と非線形変換計算部からの出力とをビット毎に排他的論理和演算を施すことによって得られることである。本発明の他の特徴は、伝送情報（平文）を暗号化する暗号化方法であって、同期信号に同期して動作する複数段のシフトレジスタの一部もしくは全部のレジスタ値に対して暗号化鍵設定部に設定された暗号化鍵を第1の排他的論理和演算手段によりビット毎に排他的論理和演算するステップと、少なくともBen_t関数と呼ばれる多ビット入力1ビット出力のブール関数演算手段を備えた非線形変換計算部によって上記第1の排他的論理和演算手段よりの値を非線形変換するステップと、上記平文と上記非線形変換計算部からの出力とを第2の排他的論理和演算手段によりビット毎に排他的論理和演算するステップと、上記暗号文を上記シフトレジスタに入力するステップとを具備することである。

【0007】本発明の他の特徴は、暗号文を復号化する復号化方法であって、同期信号に同期して動作する複数

(4)

特開2000-101567

5

6

段のシフトレジスタの一部もしくは全部のレジスタ値に対して復号化鍵設定部に設定された復号化鍵を第1の排他的論理和演算手段によりビット毎に排他的論理和演算するステップと、少なくともBent関数とよばれる多ビット入力1ビット出力のブール関数演算手段を備えた非線形変換計算部によって上記第1の排他的論理和演算手段よりの値を非線形変換するステップと、上記暗号文と上記非線形変換計算部からの出力とを第2の排他的論理和演算手段によりビット毎に排他的論理和演算するステップと、上記暗号文を、上記シフトレジスタに入力するステップとを具備することである。

【0008】

【発明の実施の形態】以下、本発明を図示した実施形態に基づいて説明する。図1は、本発明による通信システムの一実施形態を示す構成図である。図1に示す様に、この暗号通信システムは、データストリーム（平文）を暗号化する自己同期型ストリーム暗号化方式の送信部（暗号化装置）17および暗号化されたストリーム（暗号文）を復号する自己同期型ストリーム復号化方式の受信部（復号化装置）19とから成っている。上記送信部17と受信部19とは互いに同形状のシフトレジスタ21、23を有し、同形状の非線形変換計算部23、37を共有する。すなわち、上記送信部17では、平文P₁を入力する第2の排他的論理和演算部21に第1の非線形変換計算部23が、上記第1の非線形変換計算部23に第1の排他的論理和演算部群25が接続され、上記第1の排他的論理和演算部群25に暗号化鍵設定部27および第1のシフトレジスタ29が接続され、上記第1の排他的論理和演算部21の出力C₁が暗号文として伝送されると共に上記第1のシフトレジスタ29へ入力される構成となっている。

【0009】上記受信部19では、上記出力C₁を入力する第4の排他的論理和演算部31および第2のシフトレジスタ33の間に第3の排他的論理和演算部35および第2の非線形変換計算部37が接続されており、上記第3の排他的論理和演算部群35のもう一方には復号化鍵設定部39が接続されている。そして、ここで上記送信部17と受信部19とがそれぞれ暗号化鍵設定部27、復号化鍵設定部39に同じ値を共有した場合、以下のように暗号通信が成立する。上記送信部17では、平文P₁をビット毎に入力すると同期信号に同期して暗号文C₁がビット毎に出力される。詳細を説明すると、平文P₁と上記第1の非線形変換計算部23の出力は第2の排他的論理和演算部21でビット毎に排他的論理和演算が施され、その結果は暗号文C₁として出力されると共に、第1のシフトレジスタ29の最右段に入力され、*

$$u_1 = (s_{1,1}, \dots, s_{1,n}), s_{1,j} \in \{0,1\}, (1 \leq j \leq n)$$

で表し、上記非線形変換計算部（Bent関数）23の入力を、

*上記第1のシフトレジスタ29は同期信号に同期してその記憶されている内容を1ビット左シフトする。上記第1の非線形変換計算部23には上記第1のシフトレジスタ29の各段におけるレジスタ値に対して、上記暗号化鍵設定部27に設定された値とビット毎に上記第1の排他的論理和演算部群25によって排他的論理和演算が施された値が入力され、それらが非線形変換され、結果の1ビットが出力される。

【0010】上記受信部19では、上記送信部17から送信された暗号文C₁をビット毎に入力すると同期信号に同期して平文P₁がビット毎に出力される。詳細を説明すると、暗号文C₁と第2の非線形変換計算部37の出力とは第4の排他的論理和演算部31でビット毎に排他的論理和演算が施され、その結果は平文P₁として出力される。同時に暗号文C₁は第2のシフトレジスタ33の最右段に入力され、第2のシフトレジスタ33は同期信号に同期してその記憶されている内容を1ビット左シフトする。上記第2の非線形変換計算部39には上記第2のシフトレジスタ33の各段におけるレジスタ値に対して、復号化鍵設定部39に設定された値とビット毎に第3の排他的論理和演算部群35によって排他的論理和演算が施された値が入力され、それらが非線形変換され、結果の1ビットが出力される。ここで、上記非線形変換計算部23、37はBent関数と呼ばれる多ビット（偶数ビット）入力1ビット出力のブール関数の演算部からなり、当然のことながら、両者は全く同一のBent関数に基づき構成したものである。その一例を図2に示す。すなわち、図2に示す様に、このブール関数演算部では、入力端子41～47を通じて入力されたビット値が論理積演算部49、51で論理積演算され、その後、それぞれ排他的論理和演算部53に入力され、排他的論理和演算が施され、その結果が出力端子55に出力される。また、同じ値を上記暗号化鍵設定部27および復号化鍵設定部39で共有する様にしている。

【0011】以上のように構成された自己同期型ストリーム暗号方式の通信システムにより暗号通信を行った場合、ある鍵によって生成された暗号文の系列を異なる鍵で復号した場合の系列を、平文の系列と比較した場合、その相互相関が極めて小さくなる性質を有するわけであるが、その理由について以下に説明する。いま、図1の自己同期型ストリーム暗号方式の通信システムにおける送信部において、時刻1で入力される平文をP₁、出力される暗号文をC₁、第1のシフトレジスタ29の出力を、

【数1】

.....(1)

【数2】

50

(5)

特開2000-101567

$$x_i = (x_{i,1}, \dots, x_{i,n}), x_{i,j} \in \{0,1\}, (1 \leq j \leq n) \quad \dots(2)$$

上記非線形変換計算部23の出力を、

* * [数3]

$$z_i = f(x_i) \in \{0,1\} \quad \dots(3)$$

で表したとする。ただし、nは偶数である。このとき、

* [数4]

上記暗号化鍵設定部27に設定される暗号化鍵を、

※

$$k = (k_1, \dots, k_n), k_j \in \{0,1\}, (1 \leq j \leq n) \quad \dots(4)$$

とすれば、

★10★ [数5]

$$x_i = s_i \oplus k \quad \dots(5)$$

となる。ただし、

☆ ☆ [数6]

$$s_i \oplus k = (s_{i,1} \oplus k_1, \dots, s_{i,n} \oplus k_n) \quad \dots(6)$$

であり、+は排他的論理和演算を示す。また、暗号文cは、

◆ [数7]

◆

$$c_i = p_i \oplus f(x_i) = p_i \oplus z_i \quad \dots(7)$$

によって計算される。そして、これら暗号文が第1のシフトレジスタ29に入力されるため、第1のシフトレジスタ29

*スタ29においては、その内部状態は、

*20 [数8]

$$s_i = (c_{i-1}, \dots, c_{i-n}) \quad \dots(8)$$

と表すことができる。いま、平文p_i同士が統計的にランダムであり、時間的にも相関が全くないと仮定すると、上記(7)式より、暗号文c_i同士も統計的にランダムとなり、また、時間的にも相関がないことになる。これは、いかなる情報源からの系列であってもランダムな情報源からの系列と排他的論理和演算を施せばランダムな系列となるという事実から容易に理解できる。

【0012】次に、上記受信部19において、時刻iに※

※おける上記第2のシフトレジスタ33の出力を上記送信部17と同様に上記(1)式、非線形変換計算部(Bent関数)37の入力を上記(2)式、出力を上記(3)式で表したとする。また、復号化鍵設定部39に設定される復号化鍵は暗号化鍵と同じ値で上記(4)式とする。このとき、平文p_iは次のように復号化される。

【数9】

$$p_i = c_i \oplus z_i = c_i \oplus f(x_i) \quad \dots(9)$$

上記(9)式に上記(5)、(6)式および上記(8)式を適用すれば次式を得る。

★ [数10]

★

$$p_i = c_i \oplus f(c_{i-1} \oplus k_1, \dots, c_{i-n} \oplus k_n) \quad \dots(10)$$

いま、上記復号化鍵設定部39に暗号化に用いた鍵と異なる鍵、

☆ [数11]

☆

$$k' = (k'_1, \dots, k'_n), k'_j \in \{0,1\}, (1 \leq j \leq n) \quad \dots(11)$$

を設定したとする。このとき、上記受信部19の出力p'は次式のように表される。

40◆ [数12]

◆

$$p'_i = c_i \oplus f(c_{i-1} \oplus k'_1, \dots, c_{i-n} \oplus k'_n) \quad \dots(12)$$

ここにp_iとp'の相互相関は、

* * [数13]

$$p_i \oplus p'_i = f(c_{i-1} \oplus k_1, \dots, c_{i-n} \oplus k_n) \oplus f(c_{i-1} \oplus k'_1, \dots, c_{i-n} \oplus k'_n) \quad \dots(13)$$

における1、0の出現頻度によって観測することができ、特に、1、0の出現頻度が等しければ相互相関はな※

※いことになる。上記(13)式は、

【数14】

$$(c_{i-1} \oplus k_1, \dots, c_{i-n} \oplus k_n) = (u_{i,1}, \dots, u_{i,n}) = u_i \quad \dots(14)$$

(6)

特開2000-101567

10

とおくことにより、次式となる。

* * 【数15】

$$p_i \oplus p'_i = f(u_i) \oplus f(u_i \oplus b)$$

.....(15)

ただし、

※ ※ 【数16】

$$b = (b_1, \dots, b_n) = (k_1 \oplus k'_1, \dots, k_n \oplus k'_n)$$

.....(16)

である。ここに、 f はBent関数である。Bent関数においては、以下の性質が知られている。Bent関★

★数 f においては、
【数17】

$$\sum_{x \in \{0,1\}^n} f(x) \oplus f(x \oplus a) = 2^{n-1}$$

.....(17)

なる性質がある。ただし、

$$a \in \{0,1\}^n$$

である。この事実、Seonqtaek Chee, Sangjin Lee, Kwangjo Kim著の論文、"Semi-bent functions," Advances in Cryptology ASIACRYPT'94, LNCS914, Springer-Verlag, pp.107-118, 1995. 等に記されている。

【0013】上記の事実を踏まえた上で、前に述べたよ☆

☆うに、平文 p_i 同士が統計的にランダムであり、時間的にも相関が全くないと仮定すると、 $c_1, \dots, c_{1..n}$ は統計的にランダムであり、時間的にも相関が全くないことになるから、上記式(15)における u_i もランダムとみなせることになる。従って、上記式(15)に上記式(17)の結果を適用することにより、
【数18】

$$\sum_{i=1}^n p_i \oplus p'_i = \sum_{i=1}^n f(u_i) \oplus f(u_i \oplus b) = 2^{n-1}$$

.....(18)

が得られる。これは、ある鍵によって生成された暗号文の系列を異なる鍵で復号した場合の系列と、平文の系列と比較した場合、その相互相関が極めて小さくなることを示す。従って、上記図1に示した自己同期型ストリーム暗号方式の暗号通信システムでは、ある鍵によって生成された暗号文の系列を異なる鍵で復号した場合の系列と平文の系列とを比較した場合、その相互相関が極めて小さくしなければならない条件が満たされ、暗号解読の難易度を高くすることができ、また、同じ値を共有する暗号化鍵設定部および復号化鍵設定部を設ける様にしたので、鍵の設定も容易となる。

【0014】

【発明の効果】本発明は、以上説明したように、通信システムの送信部の非線形変換計算部が、Bent関数とよばれる多ビット入力1ビット出力のブール関数の演算部であり、暗号文は、平文と非線形変換部からの出力とをビット毎に排他的論理和演算を施すことによって得、その暗号文は、同時にシフトレジスタに入力される構成となっており、受信部の非線形変換計算部も、送信部と同じBent関数と呼ばれる多ビット入力1ビット出力のブール関数の演算部であり、暗号文は、シフトレジスタに入力され、同時に、平文は、先の暗号文と非線形変

換部からの出力とをビット毎に排他的論理和演算を施すことによって得る構成となっているので、ある鍵によって生成された暗号文の系列を異なる鍵で復号した場合の系列と、平文の系列とを比較した場合、その相互相関が極めて小さくなる。また、同じ値を共有する暗号化鍵設定部および復号化鍵設定部を上記した如く設ける様にしたので、鍵の設定が容易となる等の効果がある。

【図面の簡単な説明】

【図1】本発明による暗号通信システムの一実施形態を示す構成図である。

【図2】図1に示した非線形変換計算部の一例の概略構成図である。

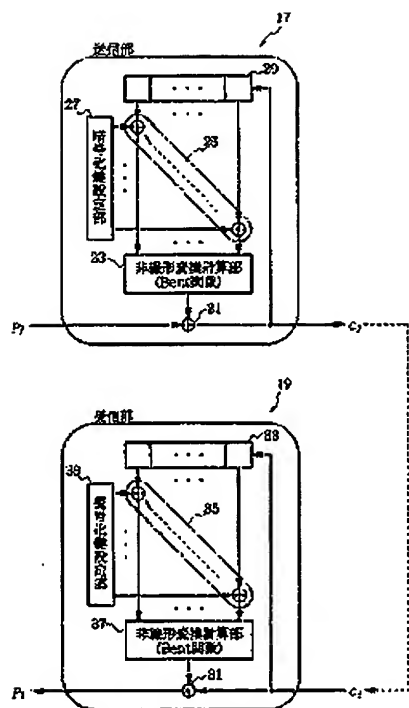
【図3】従来の暗号通信システムの構成図である。

【符号の説明】

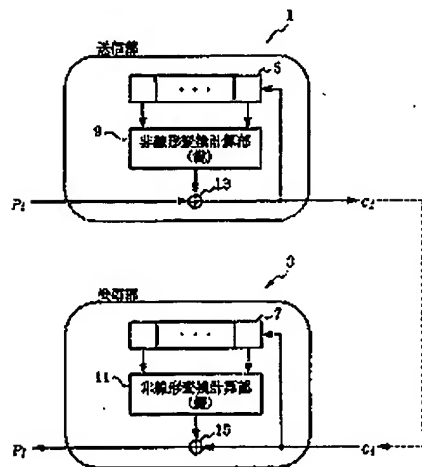
1. 17…送信部、 3. 19…受信部、5. 7. 29. 33…シフトレジスタ、9. 11. 23. 37…非線形変換計算部、13. 15. 21. 31…排他的論理和演算部、25. 35…排他的論理和演算部群、27…暗号化鍵設定部、39…復号化鍵設定部、41～47…Bent関数入力端子、49. 51…論理和演算部、53…排他的論理和演算部、55…Bent関数出力端子、

特開2000-101567

【図1】



【図3】



【図2】

